JOURNAL of PENSION BENEFITS

ISSUES IN ADMINISTRATION, DESIGN, FUNDING, AND COMPLIANCE
Volume 27 • Number 1 • Autumn 2019

PLAN DISTRIBUTIONS

Cybersecurity Should Be a Top Plan Priority

As cybercriminals find more ways to execute cyberattacks on plans and participant data, plan sponsors and providers need to assess and strengthen their plan defenses now more than ever. Plan sponsors can work with third-party auditors to evaluate plan provider processes, and establish and implement internal processes that will enhance security.

BY TERRY DUNNE

Terry Dunne is senior vice president and managing director of Retirement Services at Millennium Trust Company, LLC. Mr. Dunne has over 40 years of extensive consulting experience in the financial services industry. Millennium Trust Company performs the duties of a directed custodian, and as such does not sell investments or provide investment, legal or tax advice.

There was some surprising information in the 2019 Callan Defined Contribution Trends Survey. The results suggested retirement plan sponsors are not taking cybersecurity as seriously as they should. [“2019 Defined Contribution Trends,” Callan Institute, *https://www.callan.com/wp-content/uploads/2019/03/Callan-2019-DC-Trends-Survey.pdf* (retrieved May 2019)] According to Callan, defined contribution (DC) plans’ top five probable areas of focus for 2019 were:

1. Plan fees
2. Participant communication
3. Financial wellness
4. Fund/manager due diligence
5. Retirement readiness

The reason fees are at the top of the list is fairly clear. In recent years, a significant number of lawsuits have been filed against 401(k) fiduciaries over fees. Some have resulted in sizeable monetary settlements. Consequently, plan sponsors and service providers are painfully aware of the need to have a documented process in place and make prudent decisions when it comes to fees. [Mellman, George S. and Sanzenbacher, Geoffrey T., “401(k) Lawsuits: What are the Causes and Consequences?,” Center for Retirement Research at Boston College. *https://crr.bc.edu/wp-content/uploads/2018/04/IB_18-8.pdf* (retrieved May 2019)]

Cybersecurity came in at number 11 on the 11-item list of plan priorities for this year. Just 22 percent of plan sponsors said cybersecurity was at the top of the list. Callan's report concluded, "Despite being a newsworthy topic, cybersecurity was reported as a low priority in this year's survey."

Underestimating the importance of cybersecurity is a mistake. While the risks associated with protecting plan data have not been sharpened on the whetstone of legal action, they represent a significant vulnerability for plan sponsors. The Ponemon Institute's "2018 Cost of a Data Breach Study" reported the average price tag attached to a corporate breach was $7.91 million in the United States. ["The 2018 Cost of a Data Breach Study," Ponemon Institute, *https://costofadatabreach.mybluemix.net/?cm_mc_uid=18268543801015574295109&cm_mc_sid_50200000=28919191557429510925&cm_mc_sid_52640000=35091241557429510929* (retrieved May 2019)]

Defined Contribution Plans Are a High-Value Target for Cybercriminals

At the end of 2018, DC plans held $7.5 trillion in assets. Plans and providers also are repositories for a wealth of highly sensitive personal data, including Social Security numbers, addresses, dates of birth, account information, beneficiary data, and other records that cybercriminals actively seek. That makes plan sponsors and providers high-value targets for cybercrime. ["2019 Investment Company Fact Book," Investment Company Institute. *https://www.ici.org/pdf/2019_factbook.pdf* (retrieved May 2019)]

The Ponemon Institute's "Cost of a Data Breach Study" emphasized that the possibility of a breach is not remote. There is a greater chance a company will experience a data breach involving 10,000 or more records (27.9 percent) than there is a chance that an individual will catch the flu during the winter. The reality of data breaches is this: plan sponsors and plan providers will experience data breaches. It is a matter of when, not if.

What is important is preparing to meet the challenge. Will your plan be able to contain and eradicate the breach with minimal impact? It is critical to put protections in place so cybercriminals cannot run wild across systems, gathering data indiscriminately. Generally, that means implementing layers of security.

Securing Data Is Not Simple or Straightforward

Safeguarding plan, participant, and beneficiary data is not simple or straightforward. The United States does not have a comprehensive national law governing cybersecurity. The Department of Labor has yet to provide guidance on appropriate processes for DC plans when evaluating cybersecurity risks and/or frameworks implemented by service providers to protect data. Several states, however, such as California, New York, and Massachusetts, have implemented stricter definitions around cybersecurity practices, which only exacerbate the complexity of ensuring that DC plans follow state mandates. [Rouse, Timothy, Levine, David, *et al.*, "Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective," Pension Research Council, *https://pensionresearchcouncil.wharton.upenn.edu/wp-content/uploads/2018/12/WP-2018-16-Rouse-et-al.pdf (retrieved May 2019); "Cybersecurity Legislation 2018," National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx* (retrieved May 2019)]

Despite the lack of governance regarding cybersecurity practices, there are various resources that provide insight into the issue. The 2016 ERISA Advisory Council examined cybersecurity considerations for pension and welfare benefit plans and offered information that would help plan sponsors and providers evaluate and build cybersecurity programs. The 2016 ERISA Advisory Council's "Cybersecurity Considerations for Benefits Plans" emphasized the importance of including benefit plans in corporate cybersecurity plans:

> The 2016 Council observed that while cybersecurity is a focus area for organizations with regard to ongoing business activities, benefit plans often fall outside the scope of cybersecurity planning. Benefit plans often maintain and share sensitive employee data and asset information across multiple unrelated entities as a part of the benefit plan administration process. This data and asset information should be specifically considered when implementing cybersecurity risk management measures.

["Cybersecurity Considerations for Benefit Plans," Advisory Council on Employee Welfare and Pension Benefit Plans, *https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf* (retrieved May 2019)]

The SPARK Institute's Data Security Oversight Board (DSOB) also has provided some assistance on issues related to cybersecurity. The DSOB established best practices for third-party assessments in 2017. It recommended that plan sponsors rely on independent third-party auditors to evaluate service providers' cybersecurity systems using 16 critical data security control objectives. The DSOB also created definitions for various cybersecurity terms to make sure everyone across the industry shares a common understanding of these issues. [“Industry Best Practice Data Security Reporting” The SPARK Institute, Inc., *http://www.sparkinstitute.org/pdf/SPARK%20Data%20Security%20Industry%20Best%20Practice%20Standards%209-2017.pdf* (retrieved May 2019)]

It Is Not Prudent to Delay

With cyberattacks on the rise on multiple fronts, it is not prudent for plan sponsors to wait for guidance before taking steps to protect plan, participant, and beneficiary data. Plan sponsors need to find third-party auditors that have the knowledge to delve deeply into the 16 data security control objectives by asking service providers questions including:

- How much cybersecurity insurance do you have?
- What is your firm-wide security governance model and does it have board/executive management accountability?
- How many times do external and internal penetration tests occur?
- What types of firewalls do you have?
- What kinds of cybersecurity-related policies do you have? How often are they updated?
- What devices are connected to your system?

In addition, auditors should ask for evidence to support the answers. For instance, a company might be asked to provide:

- Sample sets of policies
- Test results from the last disaster recovery test
- High level attestations from a third party
- The name of the external network penetration test provider
- ISO or specific security certifications
- System Organization Controls (SOC) report on security practices

The ideal would be establishing a standardized set of comprehensive due diligence questionnaires that span all areas of cybersecurity, including tools, processes, test results, vendor management programs, remediation management, incidence response, and all these different pieces. A standardized questionnaire could streamline the process and allow companies to respond in a uniform manner.

Plan sponsors also should review internal processes. How is sensitive plan and personal data being safeguarded within the company? Key issues to consider include:

- **General security infrastructure**. IT departments can review the security infrastructure supporting benefits programs, including antivirus and anti-malware software and active firewalls, with an eye toward plugging any gaps. The reality is the system is likely to be breached at some point. Before that occurs, there is an opportunity to put multiple layers of security in place to contain any breach.
- **Data architecture**. Having a monolithic system that contains personal data, as well as account information, all in one place is a poor idea. Best practices for data architecture may be to not have contact information—names, addresses, phone numbers, and other personal data—in accounting systems at all. Instead, have a unique identifier in the accounting system that can be correlated to an individual whose personal data is maintained in a separate client relationship management system. If the accounting system is breached, the account data is not associated with names. If the contact system is breached, the names and other private information are not associated with account data.
- **Data protection**. Carefully review the way your company secures private personal information. Are Social Security numbers masked? Is non-public private information masked? Who has access to the information? Does the company have a written set of rules and permissions regarding access? For instance, some companies require employees who work with accounts and personal data to leave employees’ personal devices and phones in lockers before coming into client service areas.
- **Compartmentalization by job function.** Best practice is the Principle of Least Privilege (PoLP), which limits access to data. It is a robust rules-based permission system designed to ensure that only employees who need to access specific data and files to do their work are given access to only those data and files. [Lord, Nate, “What is the Principle of Least Privilege (POLP)? A Best Practice for Information Security and Compliance,” *Digital Guardian*, *https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance* (retrieved May 2019)]

- **Authentication processes**. Authenticating that people are who they say they are has become more challenging with every data breach. Historically, authentication mechanisms have relied on knowledge-based factors—information only an accountholder would know. However, data breaches have made much of this information available on the Dark Web and elsewhere. Companies should have thorough and up-to-date authentication procedures that are documented and consistently implemented.
- **A security-minded corporate culture.** A critical layer of protection for every company is its staff and training. Anyone with email should be trained to recognize and defend against email cyberthreats, such as phishing and spear-phishing attacks, and tests should be run to make sure the training is effective. Training and testing also should focus on the many other potential cyberattacks such as malware, rogue software, and "man in the middle" attacks to name a few.

A top priority for plan sponsors should be establishing, implementing, and documenting processes for protecting plan, participant and beneficiary data. Plan sponsors should review internal processes and work with third-party auditors to evaluate the processes plan providers have in place. Because cyberattacks evolve, so must plan defenses. Cybersecurity is critical for companies throughout the retirement services industry, and it will remain so into the foreseeable future. ■

Wolters Kluwer